

УГОЛОВНО-ПРАВОВЫЕ НАУКИ

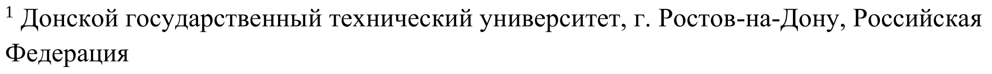
УДК 343.3

https://doi.org/10.23947/2949-1843-2023-1-4-46-57

Научная статья



Кибертерроризм как реальная угроза национальной безопасности Российской Федерации



С.И. Кузина[1, 2], **И.Г. Сагирян**[1]

[1] Донской государственный технический университет, г. Ростов-на-Дону, Российская Федерация

[2] Южно-Российский институт управления — филиал Российской академии народного хозяйства и государственной службы при Президенте РФ, г. Ростов-на-Дону, Российская Федерация



sagiryan@yandex.ru

Аннотация

Введение. В условиях стремительно меняющихся реалий, глобальным образом влияющих на нашу жизнь, на фоне проводимой Россией специальной военной операции на Донбассе остро встали вопросы терроризма во всех его разновидностях. Такого безапелляционного вызова со стороны преступно настроенной идеологии наша страна не знала со времен холодной войны. Информационные вызовы и угрозы достигли таких размеров, что уже с начала XXI века в российском правовом поле стали говорить об информационных преступлениях, информационных войнах и информационном терроризме. В связи с этим возникает потребность во всестороннем и последовательном изучении структурной организации современных преступных террористических сообществ в киберпространстве. Это позволит установить потенциальные возможности распространения идеологической пропаганды через информационно-коммуникационную сеть Интернет, установить схему финансирования кибератак на критически важные объекты инфраструктуры государства, изучить методы и технологии осуществления преступлений террористической направленности в киберпространстве. Актуальность исследования кибертерроризма определяется широким внедрением информационных технологий в национальную экономику и деятельность органов государственного управления, уязвимостью программного оборудования перед киберугрозами, развитием международной хакерской системы, совершенствованием уровня организации современных террористических группировок. Целью исследования является формирование представления о кибертерроризме, выявление причин появления и определение специфики современных киберпреступлений террористической направленности в условиях перехода к многополярному миропорядку.

Материалы и методы. Объектом исследования является кибертерроризм и общественные отношения, возникшие вследствие установления и реализации уголовно-правовых мер противодействия кибертерроризму. В исследовании был применен диалектический метод познания как основной, общенаучные методы анализа, синтеза, специальные юридические методы — эмпирические (обобщение судебной практики, уголовно-статистический) и формально-юридический.

Результаты исследования. Проанализировано современное состояние кибертерроризма, его место в структуре преступлений террористической направленности, посягающих на национальную безопасность Российской Федерации. Рассмотрены положения нормативных документов о противодействии кибертерроризму. Даны обоснованные выводы о причинах возникновения и распространения террористических преступлений в киберпространстве.

Обсуждение и заключение. Выводы, сделанные в результате исследования, призваны дополнить и расширить научное знание о сущности кибертерроризма, причинах его возникновения и функционирования в современных геополитических реалиях, уголовно-правовом регулировании кибертерроризма, а также послужить основой для дальнейшего научного поиска в данной области права.

Ключевые слова: киберпространство, кибертерроризм, противодействие, угроза, национальная безопасность, террористические преступления

Благодарности. Авторы выражают благодарность рецензенту, чья критическая оценка материалов и предложения по их совершенствованию способствовали повышению качества статьи.

Для цитирования. Кузина С.И., Сагирян И.Г. Кибертерроризм как реальная угроза национальной безопасности Российской Федерации. *Правовой порядок и правовые ценности.* 2023;1(4):46–57. https://doi.org/10.23947/2949-1843-2023-1-4-46-57

Original article

Cyberterrorism as a Real Threat to the National Security of the Russian Federation

Svetlana I. Kuzina[1, 2], **Inga G. Sagiryan**[1]

[1] Don State Technical University, Rostov-on-Don, Russia

[2] South-Russian Institute of Management of Russian Presidential Academy of National Economy and Public Administration (SRIM RANEPA), Rostov-on-Don, Russia

✉ sagiryan@yandex.ru

Abstract

Introduction. The rapid change of the real-world situation is affecting our lives at a global scale and at the time of Russia carrying out the special military operation in Donbass the issues of terrorism of any kind are becoming acute. Since the Cold War times our country has not confronted such a hard-line challenge inspired by the unlawful ideology. The cybersecurity challenges and threats have reached such a scale that from the beginning of the 21st century the discussions about the cybercrimes, information warfare and information terrorism have started in the Russian legal field. In this regard, there arises the need for a comprehensive and consistent study of the structural organisation of the today criminal terrorist cyberspace communities. This will enable determining the disseminating potential of the ideological propaganda via Internet (the information and communication network), revealing the scheme of financing the cyber attacks on the critical infrastructural state facilities, and studying the methods and technologies of executing the terrorist offences in cyberspace. The research on cyberterrorism is relevant due to the widespread implementation of the information technologies into the national economy and the state administration authorities' activities, vulnerability of the software and hardware to cyber threats, development of the international hacker network, and the improved level of organisation of the modern terrorist communities. The aim of the research is to form understanding about cyberterrorism, identify the reasons and determine the specifics of the modern terrorism-oriented cybercrimes in the context of transition to the polycentric world order.

Materials and methods. The objects of the research are cyberterrorism and social relations arising from the establishment and enforcement of the cyberterrorism countermeasures in the frame of the criminal law. When conducting the study, the dialectical method of cognition was used as the main one, the general scientific methods of analysis and synthesis, as well as specific juridical methods, i.e. empirical (generalisation of judicial practice, criminal-statistical) and legalistic methods were applied.

Results. The current state of cyberterrorism and its place in the structure of the terrorist offences encroaching on the national security of the Russian Federation have been analysed. The provisions of the cyberterrorism countering regulatory documents have been studied. Substantiated conclusions about the reasons for the emergence and dissemination of the terrorist offences in cyberspace have been made.

Discussion and Conclusion. The conclusions drawn as a result of the research aim to supplement and expand the scientific knowledge about the essence of cyberterrorism, the reasons for its emergence and functioning in the modern geopolitical conditions, cyberterrorism legal regulation in the frame of the criminal law, as well as to serve the platform for further scientific research in this field.

Keywords: cyberspace, cyberterrorism, counteraction, threat, national security, terrorist offences

Acknowledgements. The authors express their gratitude to the reviewer, whose critical assessment of the materials and suggestions for their enhancement contributed to significant improvement of the quality of the article.

For citation. Kuzina SI, Sagiryan IG. Cyberterrorism as a Real Threat to the National Security of the Russian Federation. *Legal Order and Legal Values.* 2023;1(4): 46–57. https://doi.org/10.23947/2949-1843-2023-1-4-46-57

Введение. В своем выступлении на полях XV саммита БРИКС, который проходил в Йоханесбурге (ЮАР) с 22 по 24 августа 2023 г., Президент Российской Федерации В.В. Путин говорил о роли БРИКС в формировании многополярного миропорядка, о переходе к торговле в национальной валюте и межбанковской кооперации, о причинах конфликта на Украине. В числе прочих Президент РФ обозначил глобальные проблемы, которые будут обсуждаться на следующем саммите, который запланирован на октябрь 2024 г. и будет проводиться в Казани. Саммит пройдет под девизом «Укрепление многосторонности для справедливого глобального развития и безопасности». Из этого следует, что вопросы всеобщей безопасности станут краеугольным камнем международной дискуссии. В.В. Путин заявил, что Россия, в частности, будет «уделять первостепенное внимание таким остро стоящим задачам, как борьба с терроризмом и распространением террористической идеологии»[1].

Актуальность вопросов безопасности очевидна особенно на фоне последствий процессов глобализации и стремительного развития информационно-коммуникационных технологий. К числу животрепещущих вопросов мировой безопасности с полным основанием следует отнести те изменения в социально-информационной сфере, которые связаны с проявлением, распространением и ущербным воздействием деструктивных идеологий, к которым, безусловно, относится терроризм. XXI век проходит под знаком глобальной информатизации. Отрицать тот факт, что инструменты влияния на общественное сознание вышли из материального мира и перешли в информационный, невозможно. Киберпространство стало той реальностью, с которой теперь нужно считаться, изучать и искать пути рационального взаимодействия.

Эпоха тотальной информатизации, в которую мы вступили окончательно и бесповоротно, выдвинула на передний край и сопутствующие ей угрозы. Терроризм как один из видов такой угрозы постепенно перешел в киберпространство и надолго там обосновался. «Терроризм сегодня обличен в современные, технологически продвинутые формы и вовлекает адептов в свои ряды с помощью сетевых технологий, активно использующих Интернет и все его возможности» [1, с. 50]. Международные террористические организации, чья деятельность запрещена на территории Российской Федерации (Хезболла, Хамас, ИГИЛ, Исламский Джихад – Джамаат Моджахедов и многие другие), опутали своими информационными сетями весь мир. Подготовка террористических актов, провокации, вербовка новых последователей, массовое запугивание мирного населения — вот те направления деятельности террористов, в которых активно используются новейшие информационные технологии. Интернет превратился в киберпространство, где ведутся нешуточные информационные войны.

Статистика показывает, что уровень террористической преступности неуклонно растет. В 2022 году зарегистрировано 2233 преступления террористического характера, о чем говорят аналитические материалы Генеральной прокуратуры РФ. Прирост по сравнению с 2021 годом составил 4,5 %[2].

Являясь правовым государством, Российская Федерация в качестве приоритетной ставит перед собой задачу защиты основ конституционного строя, обеспечения целостности и безопасности государства. Организация, функционирование и широкомасштабное продвижение террористической деятельности в сети Интернет нарушает права и свободы граждан по пользованию СМИ и Интернетом. В этой связи правовая система государства призвана не только определить правовые и организационные основы противодействия террористической деятельности, но и установить ответственность за осуществление такой деятельности.

Целью исследования является формирование представления о кибертерроризме, выявление причин появления и определение специфики современных киберпреступлений террористической направленности в условиях перехода к многополярному миропорядку.

Материалы и методы. Кибертерроризм и общественные отношения, возникшие вследствие установления и реализации уголовно-правовых мер противодействия кибертерроризму, остаются предметом дискуссий и интересов правоведов, социологов, IT-специалистов. В предпринятом исследовании был использован диалектический метод познания, позволивший рассмотреть анализируемые объекты и общественные отношения в динамике с учетом процесса развития и изменения, выявить логическую взаимосвязь между правовыми явлениями, а также исследовать взаимодействие права и общества, причины и последствия правовых процессов. Формально-юридический метод позволил обосновать тезис о том, что кибертерроризм представляет собой относительно новый вид преступлений террористической направленности, требующий дополнительного уголовно-правового регулирования. С помощью эмпирического метода была проанализирована и обобщена судебная практика по преступлениям террористической направленности вообще и кибертерроризму в частности.

[1] *Выступление В.В. Путина на саммите БРИКС.* URL: https://www.1tv.ru/news/2023-08-23/459795-vladimir_putin_vystupil_s_ob_emnoy_rechyu_na_sammite_briks (дата обращения: 23.08.2023).
[2] *Правовая статистика.* Официальный сайт Генеральной прокуратуры Российской Федерации. URL: https://genproc.gov.ru/ (дата обращения: 16.04.2023).

Методы анализа и синтеза обеспечили систематизацию аналитического материала с последующим обобщением результатов исследования.

Результаты исследования. Говоря о терроризме вообще и о кибертерроризме в частности, необходимо выяснить прежде всего, что следует понимать под киберпространством, которое является платформой для совершения актов кибертерроризма. В юридической науке с недавнего времени используется термин «террористическое киберпространство», под которым понимается «совокупность информационно-коммуникационных технологий, применяемых для вмешательства в работу ключевых объектов государства и выведения их из строя, получения или уничтожения важной недоступной для общего пользования информации» [2, с. 142]. Среди множества преступлений, совершаемых с помощью Интернета, кибертерроризм занимает, несомненно, главенствующее положение. Существующие в науке представления о кибертерроризме основаны на определении, данном В.А. Васениным. Кибертерроризм — это «совокупность противоправных действий, связанных с покушением на жизнь людей, угрозами расправ, деструктивными действиями в отношении материальных объектов, искажением объективной информации или рядом других действий, способствующих нагнетанию страха и напряженности в обществе, с целью получения преимущества при решении политических, экономических или социальных задач» [3, с. 67].

В качестве объединяющего критерия существующих в науке точек зрения на природу и сущность кибертерроризма можно указать на то, что кибертерроризм представляет собой одну из форм терроризма как такового, отличительной особенностью которого является пространство (сфера) его действия и распространения, другими словами — информационное пространство. Средствами или инструментами воздействия на государственные органы, органы местного самоуправления, иные организации и, самое главное, на сознание представителей социума становятся информация, информационные технологии и информационные ресурсы, разновидность которых с каждым годом изменяется и усложняется.

К отличительным признакам кибертерроризма следует отнести:

– радикальность действий в достижении каких-либо целей, реализации планов, продвижении своих интересов;

– асоциальность, выражающаяся в нарушении исторически сложившихся норм поведения в цивилизованном социальном обществе;

– аморальность, связанная с неприятием признанных в обществе моральных ценностей, принципов, качеств;

– противоправность преступных деяний, подрывающая существующий баланс социальных и личных интересов людей.

Пропаганда идеологии терроризма, вербовка новых приверженцев, разного рода манипуляции с общественным сознанием в виде призывов к осуществлению противоправной деятельности получили широкое распространение в киберпространстве, что способствует быстрому распространению пагубных идей в информационно-коммуникационной среде. Информационный терроризм безапелляционно захватывает целые области киберпространства, расширяя границы своего влияния. Проникновение в глубинную суть этого явления создает предпосылки для более глубокого осмысления современного терроризма и его потенциальных возможностей в плане деструктивного воздействия на государственные институты и основы информационной безопасности. «Документы стратегического планирования в сфере обеспечения национальной безопасности РФ указывают на то, что в настоящее время именно с помощью пропаганды осуществляется идеологическое и психологическое воздействие на граждан, ведется насаждение системы идей и ценностей, чуждой российскому народу и разрушительной для российского общества» [4, с. 29].

Виртуальное пространство Интернета до такой степени прочно вошло в жизнь простых людей, что представить современную жизнедеятельность без него невозможно. Этим обстоятельством мгновенно воспользовалась целая армия деструктивно настроенного элемента для достижения своих преступных целей. «По своему функциональному назначению киберпространство, в том числе информационно-телекоммуникационная сеть Интернет, сегодня по многим параметрам является наиболее привлекательным средством для экстремистско-террористической деятельности» [5, с. 100]. По подсчетам Национального антитеррористического комитета Российской Федерации, в настоящее время в мире действует более 5 тыс. интернет-сайтов, активно используемых террористами. Число порталов, обслуживающих террористов и их сторонников, постоянно растет. Этот процесс систематизирован до такой степени, что проконтролировать деятельность уже известных кибертеррористических группировок, а тем более запеленговать возникновение новых объединений представляет собой архисложную задачу, с которой спецслужбы и правоохранители сталкиваются ежечасно. Этот вид деструктивной деятельности в пространстве Интернета развивается очень быстро, можно сказать — стремительно.

По своей природе Интернет представляет собой идеальное поле для деятельности террористических организаций. Всемирная паутина привлекательна, так как обладает «легкой доступностью; незначительным или полным отсутствием национального контроля в форме законодательных норм ограничения или цензуры; неисчерпаемой аудиторией во всем мире; анонимностью общения; быстротой передачи информации; недорогой установкой, содержанием и техническим обслуживанием средств передачи информации; достаточно простым программным обеспечением интерактивной среды в сфере мультимедиа; применением традиционных средств массовой информации» [5, с. 101]. Метафоричное наименование Интернета всемирной паутиной вполне себя оправдывает. Для людей, у которых весьма примитивное представление о морали и нравственности, человек как личность не является ценностью. Интернет представляет собой очень удобный способ продвижения псевдоидеалов войны, насилия, устрашения, смерти. Подобно пауку, организатор террористического сообщества (группы) находится в центре ядра организации, опутанной многочисленными нейросетями, компьютерными ловушками. Добраться до него крайне сложно, поэтому террористы в киберпространстве чувствуют себя неуязвимыми, недосягаемыми и безнаказанными.

Информационный терроризм или кибертерроризм обладает целым рядом специфичных черт:

– наличие политического или идеологического мотива, служащего рычагом воздействия на политические и экономические государственные структуры;

– базой для возникновения и развития кибертерроризма является информационное пространство Интернета, в котором использование информации, ее распространение с использованием информационных технологий и ресурсов представляет собой безграничное поле деятельности;

– в качестве инструментов и средств негативного, агрессивного, деструктивного воздействия в киберпространстве выступают новейшие информационно-коммуникационные технологии.

Преступления террористической направленности — это общественно опасные, противоправные деяния, запрещенные Уголовным кодексом РФ и (или) Кодексом РФ об административных правонарушениях, которые оказывают воздействие или способствуют оказанию воздействия на принятие решения или совершение действия (бездействия) органом власти, органом местного самоуправления, международной организацией, социальной группой, юридическим или физическим лицом. «Использование информационных телекоммуникационных технологий в качестве орудия или средства преступного посягательства на любые объекты повышает эффективность преступной деятельности, придавая ей качественно новую форму, делая ее трансграничной, масштабной и труднораскрываемой» [6, с. 129].

Адепты кибертерроризма неустанно ищут нетривиальные способы вербовки в свои ряды новых приверженцев. Наравне с психологической атакой, угрозой и устрашением появилась еще одна форма — вербовка через телефонных мошенников (бич современности). Схема вербовки по своей сути довольно проста. Сначала мошенник всеми известными ему способами подбирается к финансовым средствам потенциальной жертвы, завладевает ими и затем предлагает вернуть их, но при условии выполнения определенных действий: совершение поджога, например, военкомата, отдела МВД, другого общественно значимого учреждения, диверсия на железной дороге, перенос пакета со взрывчаткой в места массового скопления людей. Безжалостность и беспринципность террористов пределов не имеет. Жертва соглашается на исполнение указанных или иных действий, осуществляет их и в случае успеха получает денежные средства. Другой вариант схемы выглядит приблизительно так же, но в качестве субъектов вербовки выступают подростки, которые хотят подработать, или пенсионеры, желающие поправить свое материальное положение. Телефонные мошенники звонят и предлагают осуществить то или иное преступное действие за вознаграждение. На территории Российской Федерации такие способы вербовки граждан используют спецслужбы Украины. Осуществление терактов в отношении органов власти или объектов важной инфраструктуры руками детей и стариков — их излюбленная тактика. Вербовка происходит в соцсетях. Украина регулярно мониторит сообщества молодежи, спящие ячейки и неонацистские организации, часто шантажирует граждан компроматом. Россиян толкают на террористические преступления, чтобы раскачать обстановку протестного движения в стране.

Материалы судебной практики за последние годы свидетельствуют о том, что террористическая деятельность осуществляется активно в виде пропаганды и навязывания идей ненависти и вражды в социальных сетях. Приоритетными формами представления информации террористического содержания в сети Интернет являются видеозаписи, графические изображения, аудиозаписи.

В том, что касается современного состояния киберпреступности в осуществлении террористической деятельности, особенно в то время, когда Россия проводит специальную военную операцию на Украине, то совершенно очевидным выглядит факт того, что использование новейших информационных технологий превратили военную операцию в так называемую войну дронов. Управление этими современными аппаратами осуществляется специалистами в области компьютерных технологий, которые находятся за сотни километров от

зоны боевых действий. При этом средством управления дронами выступают компьютер, беспрепятственный выход в киберпространство и спутниковое наведение.

Несмотря на значительное количество и рост преступлений террористической направленности, совершаемых в Интернете, на научно обоснованный факт объективного наличия кибертерроризма, в современном уголовном законодательстве России это понятие отсутствует. Законодатель устанавливает уголовную ответственность только за совершение террористического акта, предусмотренного ст. 205 УК РФ. До настоящего времени не установлен квалифицирующий признак, связанный с совершением теракта в киберпространстве. Это значит, что кибертерроризм не нашел в нашей юридической системе достаточного основания для его урегулирования.

Понятие «кибертерроризм» является производным от «компьютерного терроризма» и предусматривает использование в террористических целях компьютерных, телекоммуникационных, информационных высоких технологий с использованием сети Интернет. Самым распространенным на сегодняшний день проявлением кибертерроризма является кибератака (или кибератаки), представляющая собой мотивированный акт часто политического характера с целью создания потенциальной опасности для жизни и здоровья людей, нанесения значительного ущерба материальным объектам и инфраструктуре, наступления общественно опасных последствий и привлечения внимания к требованиям террористов.

Вопросы терроризма нашли отражение в нормативно-правовой системе, включающей в свою структуру ряд основополагающих документов международного уровня, в которых содержатся правовые подходы к противодействию терроризму. К нормативным актам, принятым международным сообществом в целях предупреждения терроризма, относятся, в первую очередь, соответствующие конвенции ООН:

– Международная конвенция о борьбе с захватом заложников;
– Международная конвенция о борьбе с бомбовым терроризмом;
– Международная конвенция о борьбе с финансированием терроризма;
– Шанхайская конвенция о борьбе с терроризмом, сепаратизмом и экстремизмом;
– Конвенция Совета Европы о предупреждении терроризма и др.

Международными актами в основном закреплено, что терроризм ни при каких обстоятельствах не может быть оправдан. При этом никакие соображения не берутся в расчет, будь то философские течения, религиозные воззрения, политические устои и др. Виновные в совершении террористических преступлений, и в особенности террористических актов, будут обнаружены, преступления расследованы, а наказание неминуемо в соответствии с законодательством того или иного государства.

К другим международным актам следует отнести важный по своей значимости документ. Это декларация, содержащаяся в резолюции 51/210 Генеральной Ассамблеи ООН от 17.12.1996, указывающая на безоговорочное осуждение актов, методов, практики терроризма. В ней, в частности, говорится, что государства обязаны оказывать друг другу содействие в области международного права и тесно взаимодействовать в деле предотвращения терроризма в каких бы формах он не проявлялся. Принцип недопустимости выполнения политических требований террористов закреплен в международных документах.

Правовая основа противодействия терроризму в Российской Федерации представлена целым рядом взаимосвязанных нормативных актов, во главе которых находится Конституция РФ, которая составляет правовую основу противодействия терроризму. «Конституция РФ содержит императивное правило, согласно которому общепризнанные принципы и нормы международного права и международные договоры Российской Федерации являются составной частью ее правовой системы» [7, с. 86]. Следующим по значимости является Федеральный закон от 06.03.2006 г. № 35-ФЗ «О противодействии терроризму»[3], в котором отражены основные аспекты борьбы с терроризмом на территории Российской Федерации. Уголовный кодекс РФ[4] (далее — УК РФ) закрепил уголовно-правовое обеспечение противодействия терроризму статьями 205, 205.1, 205.2, 205.3, 205.4, 205.5, 206, 208, 211, 220, 221, 277, 278, 279, 360 и 361. Ответственность за совершение преступлений террористической направленности предусмотрена статьями: 205, 205.1, 205.2, 205.3, 205.4, 205.5, 206, 208, 211, 220, 221, 277, 278, 279, 360 и 361 УК РФ.

[3] *О противодействии терроризму*. Федеральный закон № 35-ФЗ от 06.03.2006. URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102105192 (дата обращения: 24.08.2023).
[4] *Уголовный кодекс Российской Федерации.* № 63-ФЗ от 13.06.1996. URL: http://pravo.gov.ru/proxy/ips/?docbody&nd=102041891 (дата обращения: 24.08.2023).

Серьезным документом является Комплексный план противодействия идеологии терроризма в Российской Федерации на 2019–2023 годы[5]. В качестве приоритетных задач, на которые направлены мероприятия Комплексного плана, является совершенствование мер информационно-пропагандистского характера и защиты информационного пространства Российской Федерации от идеологии терроризма. В части совершенствования мер информационно-пропагандистского характера и защиты информационного пространства РФ от идеологии терроризма Комплексный план предлагает мониторинг сети Интернет на предмет выявления интернет-ресурсов, содержащих террористические материалы. При этом целесообразно использовать автоматизированные системы детектирования запрещенной информации, осуществлять мероприятия по блокированию распространения в сети Интернет террористических материалов. Исполнителем мероприятий назначены Роскомнадзор во взаимодействии с МВД России и ФСБ России.

В Российской Федерации принят ряд нормативных актов, регулирующих отношения, связанные с информационной безопасностью. Одним из них является Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г. № 149-ФЗ[6]. 30 ноября 2020 г. Парламентской Ассамблеей Организации Договора о коллективной безопасности (ОДКБ) принята Концепция плана действий и инструментария в вопросах противодействия кибервызовам и угрозам. Базовым документом по информационной безопасности в России является «Доктрина информационной безопасности Российской Федерации»[7] (утв. Указом Президента РФ от 5 декабря 2016 г. № 646), которая представляет собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной среде. Другим важным документом стала Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы[8].

Из современных правовых документов в области кибербезопасности выделяют следующие:

– Указ Президента Российской Федерации от 15 января 2013 года № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»;

– Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, утвержденная Президентом РФ от 12 декабря 2014 г. № К 1274;

– Федеральный закон от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской федерации».

Фундаментальным документом, который может стать определяющим в установлении направления кибербезопасности, является «Концепция стратегии кибербезопасности Российской Федерации». В настоящее время документ существует в проекте. Полагаем, что своевременность появления этого документа не вызывает сомнения. В документе обозначена актуальность разработки Стратегии, основанная на наличии объективных угроз со стороны стремительно развивающихся информационных и коммуникационных технологий. В Стратегии даны толкования новым терминам: информационное пространство, информационная безопасность, киберпространство, кибербезопасность. Стратегия согласуется с:

– Доктриной информационной безопасности Российской Федерации, развивая отдельные ее положения;

– Федеральным законом «Об информации, информационных технологиях и о защите информации»;

– Стратегией развития информационного общества в Российской Федерации;

– Основными направлениями государственной политики в области обеспечения безопасности автоматизированных систем, управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации;

– Основными направлениями государственной политики в области формирования культуры информационной безопасности.

---

[5] *Комплексный план противодействия идеологии терроризма в Российской Федерации на 2019–2023 годы.* Утвержден Президентом РФ 28.12.2018 № Пр-2665. Официальный сайт Национального антитеррористического комитета. URL: http://nac.gov.ru/terrorizmu-net/kompleksnyy-plan-protivodeystviya-ideologii-terrorizma-v.html (дата обращения: 24.08.2023).

[6] *Об информации, информационных технологиях и о защите информации.* Федеральный закон № 149-ФЗ от 27.07.2006. URL: http://pravo.gov.ru/proxy/ips/?docbody&nd=102108264 (дата обращения: 24.08.2023).

[7] *Доктрина информационной безопасности Российской Федерации.* Утверждена Указом Президента РФ № 646 от 05.12.2016. URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102161033 (дата обращения: 24.08.2023).

[8] *Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы.* Утверждена Указом Президента РФ № 203 от 09.05.2017. URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102431687 (дата обращения: 24.08.2023).

Кроме этого, Стратегия содержит положения, связанные с определением целей, принципов, приоритетов в обеспечении кибербезопасности.

Уровень технологической оснащенности современных террористических организаций достиг такого высокого уровня, что участники этих преступных организаций почувствовали себя властителями мира. Использование IT-технологий в деятельности террористических организаций стало делом настолько привычным, что остальные виды террористической деятельности в некотором смысле отошли на второй план. Динамика преступлений, совершаемых в сети Интернет, неуклонно растет, и прогноз таков, что терроризм сначала постепенно, а затем стремительно и окончательно обоснуется в киберпространстве. Выгоду от подобной преступной деятельности кибертеррористы уже почувствовали, и, как показывает опыт, отказываться от столь привлекательных методов устрашения общества и посягательства на безопасность государства они не станут. Это означает, что законопослушным гражданам и государству в целом брошен вызов, на который необходимо ответить на таком же высоком информационно-технологическом уровне. Пока в этой неустанной борьбе закон и порядок проигрывают. Однако в соответствии с моральными принципами, принятыми в обществе, в этой борьбе одержит победу тот, кто приложит для этого максимум усилий. С точки зрения морали, общественная безопасность и общественный порядок — это непререкаемые ценности.

Как уже было сказано выше, кибертерроризм по своей внутренней сути мало чем отличается от терроризма в традиционном понимании. Разница заключается в том, что проявления кибертерроризма имеют место в информационно-коммуникационной среде, которую другими словами можно назвать виртуальная сфера, киберпространство, Интернет. По структуре кибертерроризм представляет собой атаки и угрозы совершения таких атак на компьютерные системы, информационные сети и их внутреннее содержание. Методы, которыми пользуются кибертеррористы, не отличаются особым разнообразием. Это приемы запугивания, устрашение и принуждение органов государственной власти к выполнению нужных для террористов действий, что составляет суть террористической угрозы. Это виртуальные блокады, атаки на сервисы пользователей и их электронные почты, взломы компьютеров и целых компьютерных систем, заражение их вирусами и др. Цели, которые преследуют кибертеррористы, касаются в основном политических и экономических структур. Конечная цель любой террористической атаки, где бы она ни проводилась, — это насаждение гнетущего страха иногда с необратимыми последствиями.

С точки зрения криминологической науки, необходимо разобраться в причинах возникновения кибертерроризма, особенностях его жизнестойкости и условиях существования. В этом смысле нам импонирует точка зрения профессора А.В. Серебренниковой, которая на основе системного анализа проблемы выявила причины кибертерроризма и киберпреступности. К первой причине относится «фактически неограниченная возможность их финансирования со стороны лиц, имеющих политический, корыстный или иной интерес в достижении целей данных преступлений» [8, с. 49]. До недавнего прошлого правоохранительные органы довольно успешно справлялись с такого рода преступлениями. Однако со стремительным развитием информационных технологий одних только знаний в области криминологии и криминалистики оказалось недостаточно. Сейчас правоохранителям не удается достаточно быстро отследить финансовые потоки, а тем более пресечь их. Цель финансирования кибертерроризма в основном сводится к решению определенных политических задач. Источники финансирования, как правило, различны. Это могут быть как частные лица, так и транснациональные корпорации, орудующие на территории других государств. Мотивы финансирования имеют идеологическую основу. Важно заметить, что финансирование кибертерроризма способствует сокрытию элементов теневой экономики, т. е. прикрывает преступную деятельность отдельных субъектов. В любом случае в результате такой деятельности наблюдается подрыв экономики в виде изменения финансового микроклимата государства. Кибертеррористы отдают себе отчет в том, что экономика развитых государств сейчас полностью зависит от информационно-телекоммуникационных сетей, поэтому основную кибератаку направляют именно на информационный сектор экономики. Тем не менее основными мотивами преступников, занимающихся кибертерроризмом, остаются политические и финансовые мотивы.

Ко второй причине распространения кибертерроризма А.В. Серебренникова относит экономическую. Причина состоит «в дешевизне по сравнению с «традиционными» террористическими методами» [8, с. 49]. Оружие, взрывчатка, спецоборудование, обмундирование — все это стоит очень дорого. Кибертеррористу это не нужно, этими материалами он не пользуется. Ему достаточно получить доступ к персональному компьютеру с выходом в Интернет и запустить хакерскую атаку или вредоносный вирус, чтобы нанести значительный ущерб информационно-телекоммуникационной системе государственного органа, банковской структуры и др. В

наличии опасных программ в арсенале кибертеррориста сомневаться не приходится. Они имеются в количестве, достаточном для причинения вреда.

Третьей причиной распространения кибертерроризма А.В. Серебренникова считает его анонимность. «Как правило, лица, осуществляющие кибертеррористическую деятельность, используют псевдонимы или используют гостевой доступ к ресурсам, в которых предполагают распространение информации или вредоносных программ» [8, с. 49]. Анонимность позволяет скрыться в виртуальном пространстве так, что найти злоумышленника практически невозможно. Впрочем, анонимность всегда была визитной карточкой Интернета. Этой особенностью киберпространство и привлекает потенциальных преступников, среди которых кибертеррористы занимают ведущие позиции. В отличие от реальной действительности, где идентифицировать субъекта преступления можно по документам, видеокамерам постоянного слежения, на приграничных контрольно-пропускных пунктах и таким образом пресечь его преступные намерения или задержать, то в киберпространстве сделать это практически невозможно. Анонимность сети создает дополнительные и очень серьезные барьеры при обнаружении и задержании преступника. В случаях, когда все же удается задержать киберпреступника, то доказать, что это именно то лицо, которое находится в розыске, тоже бывает крайне сложно. Лицо однозначно будет отрицать свою причастность к совершению террористических преступлений.

Четвертая причина, по мнению А.В. Серебренниковой, заключается «в многообразии целей, которые возможно достигнуть методами кибертерроризма. <…> Разнообразие и сложность потенциальных целей кибертеррористов гарантирует возможность нахождения слабых мест и уязвимостей» [8, с. 49]. С этим утверждением нельзя не согласиться, потому что целями кибертеррористов могут стать органы государственной власти, военные объекты, банковские системы, инфраструктурные объекты, имеющие стратегическое значение. Удар по таким объектам будет ощутим настолько, насколько это сравнимо с объявлением войны.

Пятая причина распространения кибертерроризма, по мнению А.В. Серебренниковой, «состоит в широком охвате практически неограниченной публики». Глубинная суть последней причины кроется в потенциальных возможностях современных информационно-телекоммуникационных систем. С их помощью можно распространить идеологию терроризма в короткие сроки среди огромного количества людей. Пока правоохранительные органы и спецслужбы разберутся в сущности той или иной кибератаки, преступная цель кибертеррористов будет достигнута.

Прогнозы на будущее неутешительны. Эксперты выделяют высокую вероятность использования мутирующих вирусов. Опасность заключается в том, что эти вирусы постоянно меняются и не обнаруживаются традиционным инструментарием. Ожидаются мощные кибератаки на государственные сети. Вызывает обеспокоенность введение в эксплуатацию сетей пятого поколения (5G). Среди основных проблем 5G — слабая защищенность компьютеров. Увеличится количество атак на облачные сервисы хранения данных, мессенджеры, социальные сети, и наконец, повсеместное распространение медицинских устройств, работающих с беспроводными сетями[9].

В последнее время участились случаи кибератак на портал Госуслуги. Злоумышленники подделали эмблему портала, звонят по WhatsApp гражданам и сообщают о том, что их аккаунт на Госуслугах взломан, поэтому необходимо в срочном порядке принять меры по устранению неполадок. Уверенный голос скороговоркой дает указания клиенту о выполнении соответствующих действий: сообщить номер СНИЛС, сообщить код, который пришел в виде СМС-сообщения на телефон клиента. Маневренность и быстрота реакции злоумышленника не позволяет клиенту прийти в себя и начать логически рассуждать. Вся работа с клиентом сопровождается звуком работающей клавиатуры и фоновыми голосами мнимых работников портала Госуслуг. Следующим шагом злоумышленник передает клиента некоему менеджеру, который продолжает работу по «зомбированию» клиента. В результате гражданин как по мановению волшебной палочки передает неизвестному лицу персональные данные и только после этого приходит в себя. Есть все основания относить подобный вид мошенничества к кибертерроризму, потому что в конце такой обработки человек испытывает страх за то, что его персональные данные окажутся у преступника и будут использованы в чьих-то корыстных целях.

Несмотря на всестороннее противостояние государственных структур, органов местного самоуправления и правоохранительных органов этому виду преступлений, кибертерроризм, к несчастью, захватывает новые территории в виртуальном пространстве, изобретая новые инструменты для посягательства на информационную

[9] *О проекте Концепции плана действий и инструментария в вопросах противодействия кибервызовам и угрозам.* Постановление Парламентской Ассамблеи Организации Договора о коллективной безопасности № 13-5.4 от 30.11.2020. URL: https://paodkb.org/documents/kontseptsiya-plana-deystviy-i-instrumentariya-v-voprosah (дата обращения: 26.08.2023).

безопасность государства. Л.А. Бураева справедливо утверждает, что «среди всех разновидностей киберпреступлений, спектр которых стремительно увеличивается год от года, выделяют 2 основных вида кибертерроризма: первый вид, это кибертерроризм в так называемом «чистом виде», когда террористические действия совершаются с помощью компьютеров и компьютерных сетей, второй вид — это использование глобального информационного пространства в организационно-коммуникационных целях террористических групп» [9, с. 35].

Итак, всесторонний анализ причин и условий деятельности кибертеррористов позволит спрогнозировать процесс идентификации и пеленгации террористических компьютерных точек, из которых исходит кибератака. Однако такой прогноз возможен только при сплоченной и консолидированной работе разных стран. К сожалению, Россия в настоящее время оказалась в изоляции от ряда недружественных государств, не скрывающих своего желания уничтожить политическую и экономическую системы нашей страны. Поэтому основной упор на вопросы противодействия кибертерроризму необходимо делать на страны с дружественной нам политикой: Китай, Индия, Бразилия, ЮАР и др. Между тем основные причины возникновения киберугроз исходят, во-первых, из галопирующего развития информационных технологий и их внедрении в жизнь обычных людей. Во-вторых, из необратимых процессов всеобщей информатизации в мире. В-третьих, из нынешней геополитической обстановки, возникшей на международной арене между Россией и так называемым коллективным западом во главе с США.

Обсуждение и заключение. В современном российском правовом поле создано достаточное количество нормативных правовых актов, регламентирующих вопросы кибербезопасности. Однако универсального документа, который содержал бы в себе понятия, определения, цели, принципы, угрозы, меры предупреждения в области кибертерроризма, не существует. Определенные ставки делаются на концепцию существующей в проекте стратегии кибербезопасности Российской Федерации. «Проектная концепция позволила выявить государственные интересы, границы необходимой защиты и своего (государственного) присутствия в информационном пространстве» [10, с. 72]. Как будут реализованы положения концепции в будущем, покажет ее практическое применение.

С очевидностью существования кибертерроризма приходится считаться. В группу риска попало информационное пространство, через которое угроза совершения террористического акта нависла над объектами жизненно важной инфраструктуры целых государств. В данном случае важно четко осознать, что традиционные методы противодействия терроризму в киберпространстве не работают. Краеугольным камнем противостояния терроризму в Интернете должны стать консолидация мирового сообщества, борьба с самой идеологией терроризма на уровне воспитания правосознания, поиск новых информационных технологий, их скорейшее внедрение в систему поиска, обнаружения и уничтожения кибертеррористических ячеек.

Список литературы

1. Коровин В.М. Организация деятельности в сети Интернет по противодействию идеологии терроризма. *Гуманитарий Юга России*. 2019;8(6(40)):49–69. http://doi.org/10.23683/2227-8656.2019.6.2

2. Шондиров Р.Х. Киберпространство: новая платформа для терроризма. *Право и управление*. 2023;(2):141–145.

3. Васенин В.А. Информационная безопасность и компьютерный терроризм. В: *Сборник статей «Научные и методологические проблемы информационной безопасности»*. Москва; 2004. С. 67–83.

4. Алексеева М.В, Подройкина И.А. Правовой аспект формирования безопасной информационной среды, способствующей распространению традиционных российских духовно-нравственных ценностей. *Правовой порядок и правовые ценности*. 2023;1(2):24–33.

5. Лапунова Ю.А., Голяндин Н.П. Распространение идеологии экстремизма и терроризма в киберпространстве: проблемы и пути их решения. *Труды Академии управления МВД России*. 2017;3(43):100–104.

6. Витвицкая С.С., Витвицкий А.А., Исакова Ю.И. Киберпреступления: понятие, классификация, международное противодействие. *Правовой порядок и правовые ценности*. 2023;1(1):126–136.

7. Манукян А.Р. Конституционно-правовые основы противодействия терроризму. *Социально-политические науки*. 2018;(1):86–88.

8. Серебренникова А.В. Кибертерроризм: причины и условия. *Colloquium-Journal*. 2021;(17):47–49.

9. Бураева Л.А. Кибертерроризм как новая и наиболее опасная форма терроризма. *Пробелы в российском законодательстве*. 2017;(3):35–37.

10. Никипорец-Такигава Г.Ю., Бучнев Е.В. Методологические проблемы формирования концепции национальной кибербезопасности Российской Федерации. *Гуманитарные науки. Вестник Финансового университета*. 2022;12(1):70–74.

References

1. Korovin VM. Organization of Activities on the Internet to Countering the Ideology of Terrorism. *Humanities of the South of Russia*. 2019;8(6(40)):49–69. http://doi.org/10.23683/2227-8656.2019.6.2

2. Shondirov RKh. Cyberspace: a New Platform for Terrorism. *Law and Management*. 2023;(2):141–145.

3. Vasenin VA. Information Security and Computer Terrorism. In: *Collected Papers "Scientific and Methodological Problems of Information Security"*. Moscow; 2004. P. 67–83.

4. Alekseeva MV. Podroykina IA. Legal Aspect of Forming the Secure Informational Environment Fostering Dissemination of the Traditional Russian Spiritual and Moral Values. *Legal Order and Legal Values*. 2023;1(2):24–33.

5. Lapunova YuA, Goliandin NP. How to Solve Problems in Checking the Spread of Extremist and Terrorist Ideologies in Cyberspace. *Proceedings of the Management Academy of the Ministry of the Interior of Russia*.2017;3(43):100–104.

6. Vitvitskaya SS, Vitvitsky AA, Isakova YuI. Cybercrimes: Concept, Classification, International Countering. *Legal Order and Legal Values*. 2023;1(1):126–136.

7. Manykian AR. Constitutional and Legal Bases of Counteraction to Terrorism. *Sociopolitical Sciences*. 2018;(1):86–88.

8. Serebrennikova AV. Cyber Terrorism: Causes and Conditions. *Colloquium-Journal*. 2021;(17):47–49.

9. Burayeva LA. Cyberterrorism as a New and Most Dangerous Form of Terrorism. *Gaps in Russian Legislation*. 2017;(3):35–37.

10. Nikiporets-Takigawa GYu, Buchnev EV. Methodological Problems Concerning Concept's Formation of the National Cybersecurity in the Russian Federation. *Humanities and Social Sciences. Bulletin of the Financial University*. 2022;12(1):70–74.

Поступила в редакцию 14.11.2023
Поступила после рецензирования 14.12.2023
Принята к публикации 15.12.2023

Об авторах:

Светлана Ивановна Кузина, доктор политических наук, профессор, профессор кафедры «Уголовное право и публично-правовые дисциплины» Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), профессор кафедры политологии и этнополитики Южно-Российского института управления — филиала Российской академии народного хозяйства и государственной службы при Президенте РФ (344002, РФ, г. Ростов-на-Дону, ул. Пушкинская, 70), SCOPUS, ORCID, svivk@yandex.ru

Инга Григорьевна Сагирян, кандидат филологических наук, доцент, доцент кафедры «Уголовное право и публично-правовые дисциплины» Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), SCOPUS, ORCID, sagiryan@yandex.ru

Заявленный вклад авторов:

И.Г. Сагирян — формирование основной концепции, методология исследования, постановка задач исследования, подготовка текста, формирование выводов.

С.В. Кузина — обзор и анализ научных источников, доработка текста, корректировка выводов.

Конфликт интересов: авторы заявляют об отсутствии конфликта интересов.

Все авторы прочитали и одобрили окончательный вариант рукописи.

Received 14.11.2023
Revised 14.12.2023
Accepted 15.12.2023

About the Authors:

Svetlana I. Kuzina, Dr.Sci. (Political Sciences), Professor, Professor of the Criminal Law and Public Law Disciplines Department, Don State Technical University (1, Gagarin Sq., Rostov-on-Don, 344003, RF), Professor of the Political Science and Ethnopolitics Department, South-Russian Institute of Management of Russian Presidential Academy of National Economy and Public Administration (70, Pushkinskaya St., Rostov-on-Don, 344002, RF), SCOPUS, ORCID, svivk@yandex.ru

Inga G. Sagiryan, Cand.Sci. (Philology), Associate Professor, Associate Professor of the Criminal Law and Public Law Disciplines Department, Don State Technical University (1, Gagarin Sq., Rostov-on-Don, 344003, RF), SCOPUS, ORCID, sagiryan@yandex.ru

Claimed contributorship:

IG Sagiryan: formulating the main concept, research methodology, setting research objectives, preparing the text, formulating the conclusions.

SI Kuzina: review and analysis of scientific sources, refining the text, correcting the conclusions.

Conflict of interest statement: the authors do not have any conflict of interest.

All authors have read and approved the final manuscript.